The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
09/27/2019
08/13/2020 - UPDATED

SUBJECT:
A Vulnerability in vBulletin Could Allow for Remote Code Execution

OVERVIEW:
A vulnerability has been discovered in vBulletin which could allow for remote code execution when a malicious POST request is sent to the vulnerable application. vBulletin is a software package written in PHP used to create forums. Successful exploitation of this vulnerability could enable the attacker to perform system command execution in the context of the web server hosting the application. Depending on the privileges associated with the vBulletin service, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights

THREAT INTELLIGENCE:
There are reports of this vulnerability being exploited in the wild.

August 13 – UPDATED THREAT INTELLIGENCE:
A proof of concept was unveiled that would allow an attacker to bypass the previous fix.

SYSTEMS AFFECTED:

- vBulletin versions 5.0.0 to 5.5.4

August 13 – UPDATED SYSTEMS AFFECTED:

- ***vBulletin versions 5.0.0 to 5.6.2***

RISK:
Government:

- Large and medium government entities: **Medium**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **Medium**
- Small business entities: **Medium**

Home users: NA

TECHNICAL SUMMARY:

A vulnerability has been discovered in vBulletin which can allow for remote code execution when a malicious POST request is sent to the vulnerable application. This vulnerability exists due to improper input validation within the widgetConfig[code] parameter when a POST request is sent to the index page of the vBulletin with the routestring, “ajax/render/widget_php”. An attacker can load an arbitrary widget and run code provided within the widgetConfig[code] parameter. Depending on the privileges associated with the vBulletin service, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate updates provided by vBulletin to vulnerable systems, immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
vBulletin:
https://forum.vbulletin.com/forum/vbulletin-announcements/vbulletin-announcements_aa/4422707-vbulletin-security-patch-released-versions-5-5-2-5-5-3-and-5-5-4

SecList:
https://seclists.org/fulldisclosure/2019/Sep/31

Ars Technica:
https://arstechnica.com/information-technology/2019/09/public-exploit-code-spawns-mass-attacks-against-high-severity-vbulletin-bug/

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-16759

August 13 – UPDATED REFERENCES
vBulletin:
https://forum.vbulletin.com/forum/vbulletin-announcements/vbulletin-announcements_aa/4445227-vbulletin-5-6-0-5-6-1-5-6-2-security-patch